

*Interview Summary*

The applicant thanks the Examiner for the helpful interview to discuss the interpretation of the prior art and the claims as presented. In response to the applicant's explanation of the prior art, generally as presented in the response to the second Office Action, the Examiner indicated that it was not clear from the language of the claims how the claims related to the generalized embodiment of Figure 3 and as described in the application at paragraphs [0060]-[[0067]. The Examiner suggested that the applicant consider amendments by way of a RCE to clarify the scope of protection sought in the claims.

REMARKS

The applicant has amended the claims to more clearly define the scope of protection sought. In particular, the applicant has amended the preambles to specify that this is a method for improving the resistance, to power analysis attacks, of a processing unit performing a cryptographic function. The applicant has also made a voluntary amendment to the program product claims to specify that the medium is a "storage medium". This amendment is supported at paragraph [0045] and is intended to more clearly define the scope of protection sought.

As explained in the Background (paragraphs [0002]-[0011]), a device employing a processing unit to carry out a cryptographic operation may be susceptible to physical measurement of the changing voltage levels in the device as a known input is encrypted by the device. This physical measurement of the device voltage levels is known as a power analysis attack.

A power analysis attack may yield information about an operation performed by the device, or a value stored in memory on the device. Depending upon the physical layout of the device, and the way a particular cryptographic function is structured, different aspects of the operation may be more, or less, susceptible to a power analysis attack. Countermeasure methods to increase the resistance of the device to a power analysis attacks have been developed, and some are described in the background (Messerges, Kocher, Chari et al.).

The Examiner has cited US 6,278,381 (Kocher et al.), as disclosing the subject matter of the claims. The applicant respectfully disagrees.

Kocher is directed towards a masking and permutation scheme for making DES-type cryptography resistant to attack. The scheme involves replacing the key K with a random mask value K1 and a masked key K2, related to K by the relationship  $K2 = K \text{ XOR } K1$ . In Kocher, the masked key K2 is the original key K as masked by the random mask K1. The masked key K2 and mask K1 are also permuted, with random permutations created K2P and K1P.

The message is similarly modified by generating a masked message M2 by applying a random value mask M1 to the original message M. So,  $M2 = M \text{ XOR } M1$ . The masked message M2 and mask M1 are similarly permuted to generate M1P and M2P. The permuted keys and messages are then used, rather than the standard key and message in the cryptographic operation.

See generally column 2 ln 25-66, column 6 ln 29-68 and column 9 ln 1-23.

In summary, Kocher protects various values, such as the key K, using a straight masking operation ( $K2 = K \text{ XOR } K1$ ) so that a masked version of the value, in this case masked key K2, as permuted to K2P, and the mask K1, as permuted to K1P, is used in the cryptographic operation.

The present application is directed towards a method for protecting the key and key mask by using replacement values in the cryptographic operation in place of the key and key mask. The present application achieves this by using split masks, where the split masks are defined with reference to random values used in the masking operation, so that in the operation each encryption operation using the same key only the split mask values  $m1, m2, \dots, mn$  and masked key mkey are used in the operation. The key mask r is not directly applied or used in the cryptographic operation. Accordingly, measurements of the cryptographic operation through a power analysis attack will not yield the key value or the key mask value r.

To compare with Kocher, mkey is roughly equivalent to K2 and the key mask value r is roughly equivalent to K1. Unlike Kocher, however, r, or a permutation of r, is not used in the

cryptographic operation. Instead, split mask values are used, where mn is defined in relation to r, such that the r is indirectly a component of the cryptographic function.

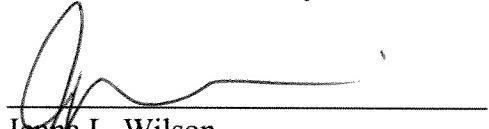
Kocher, only discloses using a permutation of K1 in the cryptographic operation. There is no disclosure in Kocher of using split masks, where mn is defined in relation to r, in the cryptographic operation.

Accordingly, the Examiner's argument that Kocher discloses defining a value mn, or obtaining a set of random values m1, ...mn-1, is incorrect. Kocher employs a permutation of K1, K1P, in the operation and does not generate a split mask defined in relation to the key mask value. The applicant would further argue that other aspects of the claim are distinguishable over Kocher. For instance, Kocher does not disclose obtaining a set of n random input values, to be used in masking a defined cryptographic function or generating a mask table.

Favourable consideration and allowance of this application are respectfully requested.

Executed at Toronto, Ontario, Canada, on October 21, 2009.

Catherine Helen Gebotys

  
Jemma L. Wilson  
Registration No. 54908  
(647) 288-9532

**Customer Number: 38735**

JLW:iw  
Request for Continued Examination (RCE)